

侵入の痕跡 (Indicators of Compromises, IoCs)

SORA (SHA-1)

- 35b0d5dbcaba3edd0d7b3e7b14b36cb96527148c
- 4bbe4ec21a148000838b66a334e956944797eeab
- 8d8b01e3fc145a1f64eed6d39bdf5db2d8fbec60
- abaf3640c849a4bc32304a40f9bf0adaeef8c893
- bd37f93e284cf2b7d9320808b50ed98cd6d0ffa3
- c2809d998c267a1a24660ca7f33becb86f5b02ce
- d56d2e59185b19b5a06ae1dc2652c3eb856c005b
- f86fe270ff7a1502a3fbce8aa148a13cbe194a92
- fa17c4545946027f11c8fb7c5a4f08ff8f26ce75

UNSTABLE (SHA-1) (UX で圧縮されているファイル含む)

- 4f11cca6f909e8bd7b5bf276da983a2a38f6a1d2
- 81e6c575a4000797d5bdfbd0048a514bb6c05001
- a019c886ba3bfa4bb3b976a620c08bb3058e257b
- 4fd05325244a6d8d0c0fa20ec9f44af9e380b653
- a792d58f42caa7ab038702cbf8f2a2de3b327131
- ac0bacf92b382de09d7a625e9f380cd2a389bccb
- 45d644aba5ea368bd366b543663dac00c72aeeee
- d7ca3bcad5cba00574f7247562597cdca0d2bead
- 8d79da230bf64f7e3be18c4d4c2837bdf76be744
- 4d5452315f5c5a742e17ab1c14e4356fd669b448

関連する不正な IP アドレスおよび URL

- IP 45.148.10.86
- IP 193.70.125.169
- hxxp://faygox.duckdns[.]org/thinkphp
- hxxp://faygox.duckdns[.]org/gpon443
- zxcxffytttygbbgfgf12121bot[.]duckdns.org
- cncctomecutie1337[.]mikeysyach[.]xyz
- scanthembigbots[.]mikeysyach[.]xyz

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information. Our innovative solutions provide our customers with layered security for data centers, cloud workloads, networks, and endpoints.

At the heart of our leadership, Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights with the public, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on targeted attacks, artificial intelligence, Internet of Things (IoT), cybercriminals, and more. We continually work to anticipate the next wave of threats and deliver thought-provoking research that can shape strategic industry direction.

www.trendmicro.com

